

# 15 Cybersecurity

## Myths

vs

## Reality

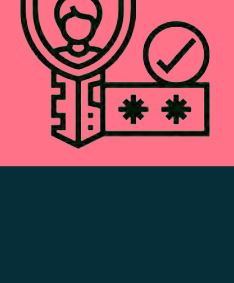
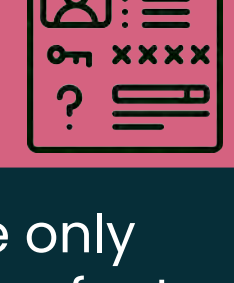


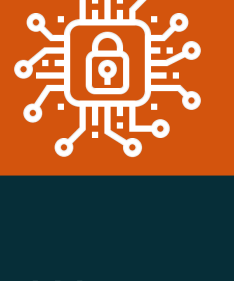



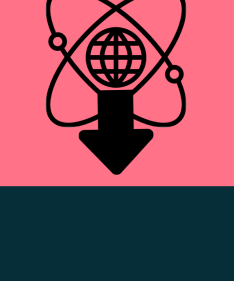



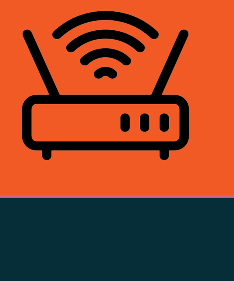



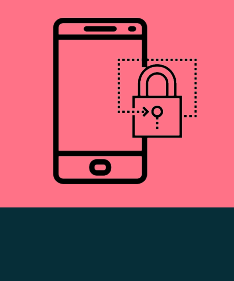
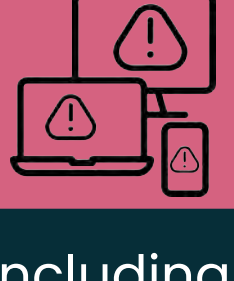






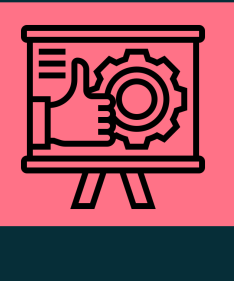





Are these cybersecurity myths and misconceptions putting your business at risk?

It's time to know the facts about cybersecurity!

### Myths

vs

### Reality

 <p>Our passwords are strong</p>	1	 <p>Strong passwords are only the start. You need two-factor authentication and data monitoring</p>
 <p>Cybercriminals don't target SMBs</p>	2	 <p>Small businesses lack advanced security solutions, making them a softer target for cybercriminals</p>
 <p>We are unlikely to experience a cyberattack</p>	3	 <p>Any business with sensitive information is highly likely to witness a cyberattack at some stage</p>
 <p>Anti-virus/anti-malware software is enough</p>	4	 <p>Software won't be able to detect/prevent all types of cyber attacks</p>
 <p>Cyberthreats are only external</p>	5	 <p>Insider threats are equally perilous and need equal attention as external threats</p>
 <p>IT department is responsible for cybersecurity</p>	6	 <p>It is the responsibility of every employee to keep the organization cyber safe</p>
 <p>Password protected Wi-Fi networks are secure</p>	7	 <p>All public Wi-Fi networks can be compromised, even with a password</p>
 <p>You'll know immediately if your system is compromised</p>	8	 <p>It can take months or even years to realize that your system has been compromised</p>
 <p>BYOD is secure and safe</p>	9	 <p>All personal devices, including smartphones, laptops, and wearables, can put a company's network at risk</p>
 <p>We have achieved complete cybersecurity</p>	10	 <p>You must continuously adopt new cybersecurity strategies as new threats emerge</p>
 <p>Sophisticated security tools keep your business secure</p>	11	 <p>Security tools should be appropriately configured, monitored, and integrated with overall security operations</p>
 <p>Regular penetration tests are enough</p>	12	 <p>Penetrations tests work only when the discovered vulnerabilities are rectified in time</p>
 <p>Compliance equates to a robust security strategy</p>	13	 <p>Merely complying with regulations does not mean you have a robust security strategy</p>
 <p>A third-party security provider will take care of security</p>	14	 <p>Despite partnering with a security provider, you have a legal and ethical responsibility to secure critical assets</p>
 <p>We have never experienced a breach, so our security is strong</p>	15	 <p>New, sophisticated cyberattacks evolve daily, so be prepared always</p>

**Want to Become a Secure, Vigilant, and Resilient Business? Stealthlabs Will Help!**



[Contact Us](#)